CHAPTER 1

INTRODUCTION

1.1 An Overview

In today's cloud computing is very important aspect in the world. Its popularity is increasing day by day, because it provides us on demand access the resources and also shared the resources such as software and hardware for efficient manage. Outsources data in public cloud decreases the control of data owner on it, and to preserve the control of data in cloud or within networks is beneficial for data security. Data duplication is also such a problem which is waste the money for data sharing and management. A keystone for remote data storage in client's side duplication, where server stores only single copy in the server's side regardless how many client want to store that file. This technique will save the cost of both of communication bandwidth as well as memory capacity.

There are many techniques are available for protecting data in cloud such as data integrity checking, data authentication, access control, encryption, data masking and so on. Cryptography is the one of the powerful technique for data security in cloud computing. This includes the design of encryption and decryption algorithm which protects our confidential data and convert it in unreadable form. Before outsourcing data to cloud server is encrypted using a novel encryption technique and decrypted later using same shared key.

Cryptographic Hash function is also a data protection technique which is used for authentication purpose. It takes a message input of arbitrary length and generates fixed length of message digest. Client side duplication is a new type of problem, in proposed model which is Solve by hashing function and give a better result than previous one.

1.2 General Concepts

Cloud system is more vulnerable to threats that that bring various types of damages resulting in endanger of human life and serious loss to major economic infrastructures. From the perspective of data security in cloud computing, data owner totally depended on third party auditor. However, there are legal effectual regulations such as the U S Health Insurance Portability and Accountability Act (HIPAA). Further, demand of outsourced not to be leaked to external parties. Use of data encryption before outsourced the data is most secure technique for confidentiality of data. In cloud computing duplication is also increasingly problem that affect the cost as well as security. Data owner become increasingly outsourced the confidential data and also check the duplication of file from cryptographically proposed scheme from local system to remote system.

In proposed system I have focused on preserving the outsourced as a security aspect and remove the duplication of storage file from client location to server location. Due to this reason I proposed a highly efficient encryption technique and hash function which is used in local server before sending the data to trusted third party auditor (TTPA). Before sending the data, date will be divided into block, and each block contains the 64 byte of data. Each block is encrypted using my proposed encryption technique and each block creates fixed number of message digest and prepares a table. Then table has sent to TTPA which contains the information of each block (such as block number, status of block and so on) and massage digest of particular block. When end user request the access the data that time request will be send over two places, at TTPA and at cloud service provider (CSP). TTPA firstly authenticates the user and sends the signal to CSP in the form of negative or positive. If signal is positive, then CSP sends the particular file to end users and TTPA will also send the particular table which stores the information regarding file. End user calculate the hash value of particular message which have got from CSP and compare that value from TTPA table which contain the hash value. If both of the value is matched then message is authenticated and then decrypt the message using decryption algorithm.

1.3 Motivation

Nowadays cloud computing is becoming an integral part of major business organisations and individuals as they are shifting their business operations, confidential data to cloud environment.

Hence it is necessary to protect this critical data and operations from the opposition and attackers and to ensure that the information within Cloud system is secure. In cloud computing data owner rely on TTPA for storage security of data, but data owner have some doubt ,is his data is secure or not?. This is the biggest question of every data owner. Confidentiality of data is the main concern in cloud system and data duplication may also lead the threats on cloud. However there are legal regulations, such as the U S Health Insurance Portability and Accountability Act (HIPAA), further demanding the outsourced data not to be leaked to external parties. This motivated us to explore the work on security impact on outsourced data and also detect the data duplication to Cloud system.

1.4 Related Work

In last decade researchers have been working on it, many researcher works on this areas and also proposed some techniques which help to give a better platform to research in my area. Our research could find only few proposals in the domain of Cloud where "Security" is a great concern. If proper measures are not taken for security in the early stages it may lead to an inefficient system or may result in a failure.

Security basically deals with protecting CIA (confidentiality, integrity and availability).

But Firesmith [22] has defined twelve different Security Requirements covering CIA as well as identification, authorization, immunity etc. He also distinguished between Security Requirements and architectural constraints so that true Security Requirements can be identified which can lead to cost effective secure system.

In literature we studied about different-different type of cryptography based security model like , OPE and FPE[7], Provable Ownership of the File (POF)[8], Hybrid Vigenere

Caesar Cipher Encryption (HVCCE)[1]. All models have proposed for security purpose in cloud environment.

There are many encryption techniques are used in server side for protection of data such as Homomorphic encryption, RSA, AES, DES, Eliptical encryption, combination of RSA and AES etc.[3,9,10 ,17]. J.P. Martin-Flatin[5] has also described the various type of challenges which will affect the our cloud environment at management time. Kirti Gupta & Dr. Shailendra Narayan Singh[4] have also describe the method for maintain the security on cloud stored data.

P.Varalakshmi & Hamsavardhini Deventhiran[18] identified the integrity of data is very important also proposed a model for the integrity checking using encryption algorithm on cloud.

Somchart Fugkeaw[21] described the technique for enhance the scalability and fine-grained access control for outsourcing data in multi owner setting. Chun-I Fan, Shi-Yuan Huang, and Wen-Che Hsu[13] described the data de-duplication and gave a solution using encryption algorithm.

Cloud computing researchers have also recognized the data confidentiality and data verification and few proposals have also focused on it [14].

Some of the researchers have also analyzed the data owner rely on TPA, If the data to be leaked on external parties, then confidentiality is to be loosed. Many researchers have focused on outsourced data and try to provide secure technique for protection purpose on cloud system , following are some work done by researchers in the field of security of outsourced data for Cloud system.

Somchart Fugkeaw[21] described the technique for enhance the scalability and fine-grained access control for outsourcing data in multi owner setting.

Fang Liu, Wee Keong Ng, Wei Zhang[12] have tried to solve storage capacity and management cost of outsourced data on cloud and proposed a novel protocol for outsourced rule mining (PROM) ,where data are encrypted and outsourced both.

1.5 Problem Statement

From the foregoing section we can conclude that there are not concrete proposals for Security of outsourced data and not a reliable technique for removing of data duplication in the domain of Cloud. Existing approaches do not consider all possible security concerns. In addition there is no framework or formal model for data security of outsourcing and accessing the confidential data in cloud environment.

Hence the problem of Thesis is

"**Propose a Cryptography based framework for data security of outsourcing and accessing the data for Cloud system and apply it to develop a secure system for Cloud Storage-as-a service model.**"

The framework has well defined steps which describe how Security preserved the all areas of cloud system in an efficient way. The proposal on protection of outsourcing the data will be useful for engineer to determine the structured way through which security can be performed on cloud system.

1.6 Scope of Work

The real motive of proposal is to provide a well defined model for security of outsourcing the data in Cloud system. Earlier proposals by researchers are very limited and also unable to consider every possible security concern in Cloud. Their proposed approaches are also not based on any process, method or framework. So we wish to extend or proposed a novel framework for security of outsourcing the data. In this proposal security is main factor which will be preserve the all areas on the cloud system as well as also try to remove the duplication of file on client side.

In this project we adapt the novel cryptographic technique before outsourcing the data in the domain of Cloud System. We then define low level Security model in the same domain. These Security models are nothing but are low level Security model which helps the design engineer to take optimal decision in implementing security model on cloud. Our process consists of identifying the Security

Requirements and then maps them to Security Functionalities. We then finally illustrate our approach for Cloud Storage-as-a-service.

Hence our work will cover:

- Eliciting different Security Requirements related to Cloud system.
- Defining Security Functionalities.
- Presenting step by step method in the perspective of security on cloud.
- Perform a case study on real world Cloud Storage services to ensure security.

1.7 Organization of Thesis

The rest of this thesis is organized as follows:

Chapter 2 provides a basic overview of Cloud computing by first giving definition and the history associated with Cloud computing. Then it describes the various models available in Cloud computing with their merits and demerits. And lastly it discusses the advantages of Cloud with some available issues.

Chapter 3 gives the overview of our study on Security of outsourcing the data. It first gives a brief idea about Security activities. Then it introduces security requirements on various places at cloud and explained the various proposed cryptographic based technique during last two decades. At last it presents Security Design Framework and Security Testing Framework proposed by researchers.

Chapter 4 describes the methodology and proposed framework which will be used in our system.

Chapter 5 contains our implementation by first giving instructions to configure and then shows some snapshots of encryption and decryption algorithm as well as hash functions.

Chapter 6 finally concludes the thesis.

CHAPTER 2

CLOUD COMPUTING OVERVIEW

In this chapter we first discuss the basic definition and history of Cloud computing. Then the various models of Cloud system with their merits and demerits are given for better understanding and finally we discuss the advantages of Cloud services with their available issues.

2.1 Cloud Definition

In most of the literatures the name Cloud computing relates to the images of clouds that are representing networks and the Internet. Cloud computing was implemented into the real world because of the pressure on IT to save money and now it became future of next generation IT. Basically, Cloud computing makes data and applications available through the Internet to the Cloud users. Cloud computing is not a new technology or a new device but it is a use of existing technology and devices in a new way. A standard definition of Cloud computing given by NIST is

*"**Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction**."* [23].

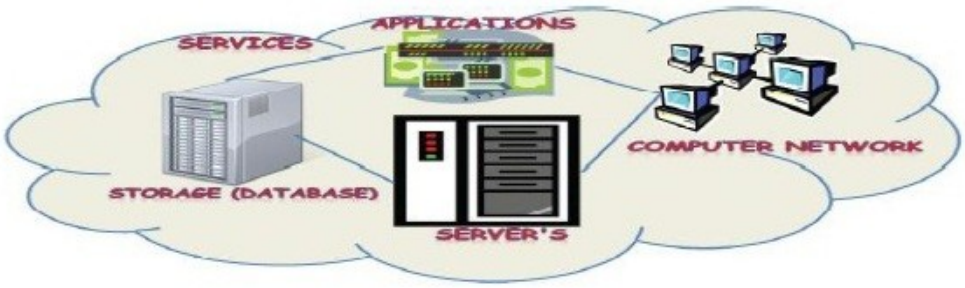


Figure 1: Cloud computing

Cloud computing architecture basically consists of hierarchical levels as shown in Figure 2.

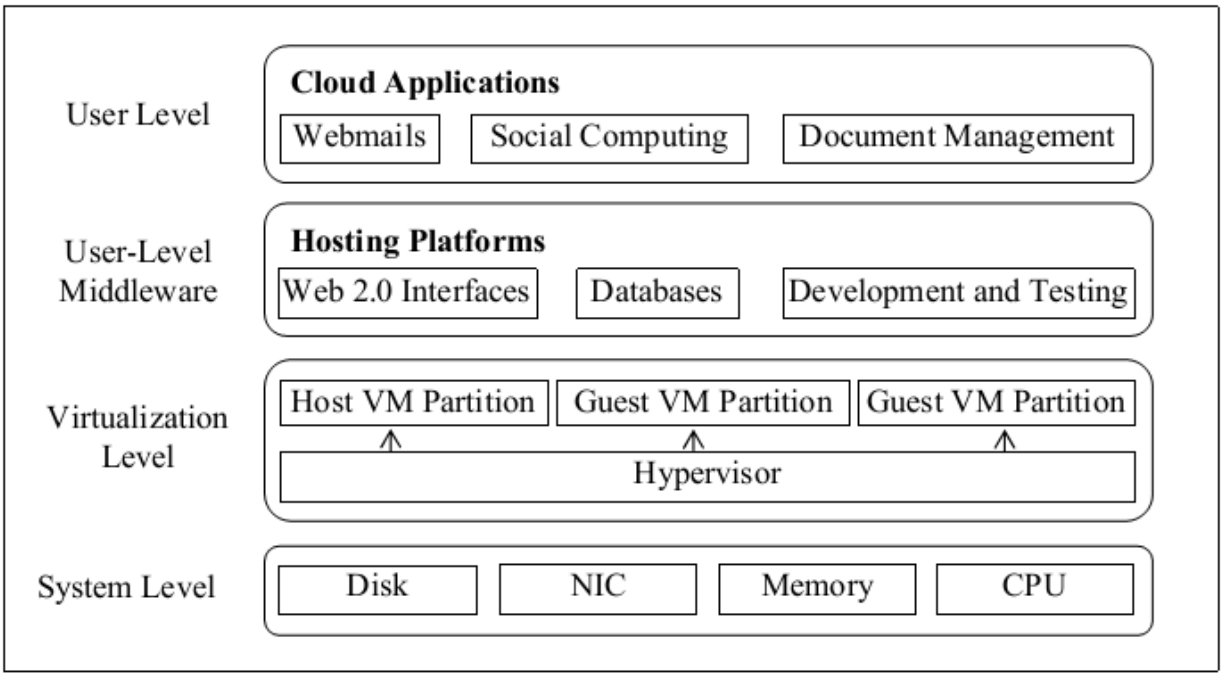


Figure 2: Cloud computing architecture

2.2 History of Cloud

John McCarthy in 60‟s said that "*computation may someday be organized as a public utility*" and today Cloud computing really seems to be breaking through. In 60‟s and 70‟s companies had large and expensive mainframe computers which provide the services to workers who access them through dumb terminals. These mainframe computers store all information and did all calculations.

Then in 80‟s these mainframes are replaced by computers for the users due to decrease in the price of personal computers. In 90‟s with the advancement of Internet technology the fashion of many computers accessing one big server came again. At that time requirement of web servers arises with plenty of powers to resolve requests that were made from the Internet. Since from that time to today numerous services are offered

in Internet with more storage capacity and massive computation requirements are solved by dedicated service providers. In this way large users can share the common infrastructure maximizing efficiency and minimizing the cost.

At the finish of 90‟s, normally all data centers were using only less than 10% of their capabilities [22] as they wanted to reserve the rest in case of occasional peaks. At this time Amazon made a great effort to solve this problem by adding capabilities on demands by the users.

In 1999 Salesforce.com began to deliver services to organizations by their own website and initiated the concept of software as a service. In 2002 Amazon launched AWS suite that includes storage, computation with other services. Again in 2006 Amazon launched EC2 for small companies and users to let them run their own computer applications in Cloud. In 2008 Eucalyptus was launched, which was the first open source AWS API compatible platform for deploying private Clouds. In 2009 Google began to offer enterprise applications as Google AppEngine. And today all large companies like Microsoft, IBM, Oracle and HP offers Cloud computing with various services.

2.3 Cloud Models

Based on the underlying infrastructure and the services offered to users, Cloud systems are classified as Cloud deployment models and Cloud service models which further consists various sub-models [23].

2.3.1 Deployment Models

In Cloud deployment models the available sub-models are public, private, hybrid and community which are distinguished by their architecture, location of datacenter and the needs of the Cloud customer.

- **Public Cloud**

Public Cloud offers the computing resources to general public over the internet via Web applications or Web browsers either on free or on pay-per-use license policy [14]. It is

advantageous as the customer does not have to buy any equipment and the resources are shared among different customers at a time. Public Cloud's physical infrastructure is owned by a CSP. Its limitation is the less control over the hardware.

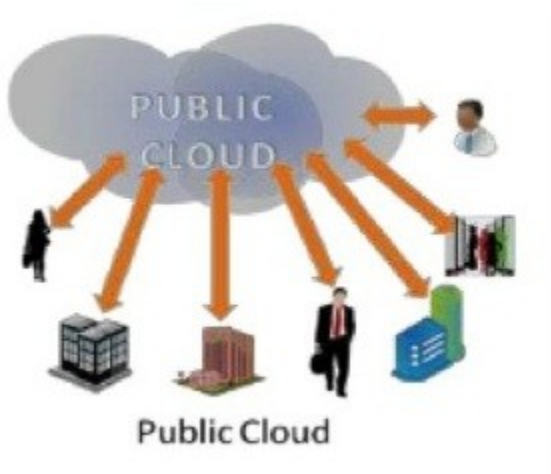


Figure 3: Public cloud

Private Cloud

It offers the infrastructure to be used by only one organization which can be located on the premises of the CSP. These are used in private networks and hence restrict the unwanted public access to the data that is used by the organization [22]. Advantage of this model is the total control over the hardware by an organization. It is also more secure than the traditional public Cloud. Its limitation is the high cost.

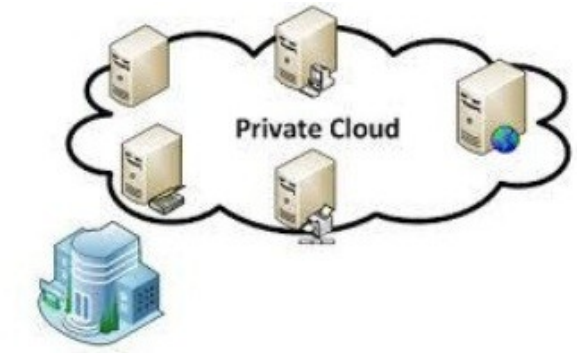


Figure4: Private cloud

 Hybrid Cloud

Hybrid Cloud consists of combination of public and private Cloud. So through its implementation an organization can benefits from the advantages of both Clouds. For example an organization can runs all applications in private Cloud and uses public Cloud when private Cloud lacks from certain features.

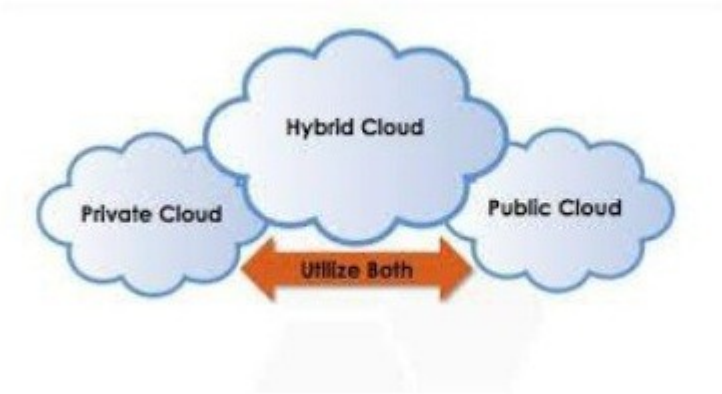


Figure 5: hybrid cloud

 Community Cloud

Community Cloud offers to share the resources and hardware between organizations that have similar needs. So it is a private Cloud for a community, where community consists of organizations fewer than public Cloud and more than private Cloud. Security of data is compromised in this model.

Figure 6: Community cloud

Hence, for deciding which type of Cloud to deploy in organization, the business managers need to assess each Cloud deployment model from multiple points of view like cost, economy, availability etc. A comparison between various Cloud deployment models with their merits and demerits are summarized in Table 1.

Table 1: Deployment models comparison

Clouds	Merits	Demerits
Public	Efficient use of hardware No need to buy hardware	Data stored off-premise
Private	Control over hardware Control over data	High cost Hardware has to be bought
Hybrid	Critical information can stay on premise	Less efficient than public cloud
Community	Cost can be spread Efficient use of hardware	Less efficient than public cloud

2.3.2 Service Models

Similar to deployment models, the service models are also sub-divided mostly into four categories as Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Storage as a Service (StaaS) [23].

- **Software as a Service (SaaS)**

In SaaS model the CSU access the application software installed and maintained by CSP at providers end. In this the implementation and deployment is abstracted from the user and only limited set of configuration control is made available by provider. Its main

benefit is the reduction in hardware cost and software development and maintenance cost. Examples of SaaS are MS Office 365, Quickbooks online and Salesforce.com.

 Platform as a Service (PaaS)

The CSP provides the computing platform as on demand service on which applications can be developed and deployed. In addition to computing platform a solution stack consists of operating systems, programming language environment, databases and web servers is also provided to customers. This model is mostly suitable for developers. Its purpose is to reduce cost and complexity of buying and managing underlying hardware and software components. Examples of PaaS are GAE, Force.com and Windows Azure Compute.

 Infrastructure as a Service (IaaS)

In IaaS model the computing infrastructure like servers, network equipment‟s and software are provided as on-demand services where the customers can install operating system images with applications to create their own customized environment. The CSP owns the hardware and is responsible for housing and maintaining them. Examples of IaaS are Rackspace Cloud, Amazon EC2, Google Compute Engine and GoGrid.

 Storage as a Service (StaaS)

In StaaS model the provider provides the storage services on their own infrastructure. Cloud storage system can be considered as a network of distributed data servers which use cloud computing features like virtualization and provide some kind of interface for storing the customer data. Basic features of Cloud storage services are copy, backup, synchronization and file sharing. Examples of StaaS are Dropbox, Mozy, and Cloud One etc. In terms of efficiency and cost, the best suitable service model is SaaS but IaaS is best related to control over hardware and data as shown in Figure 7.

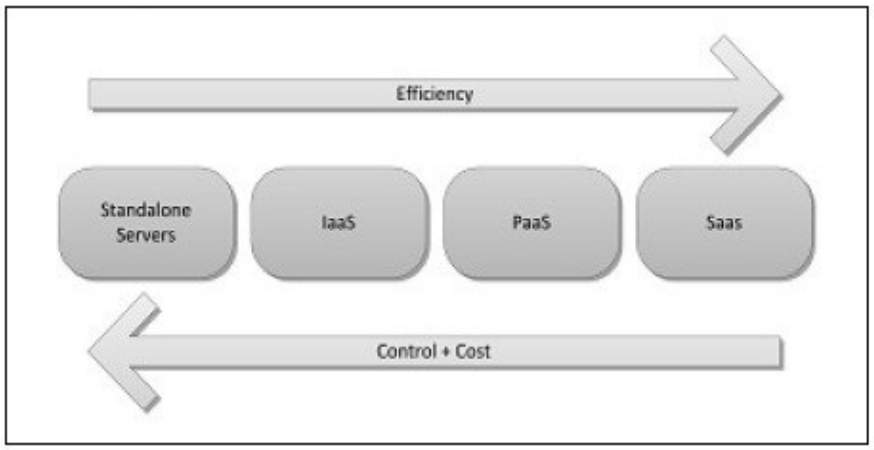


Figure 7: Efficiency & cost related to Cloud service models

2.4 Advantages of Cloud Computing

While Cloud computing is undoubtedly beneficial for mid-size to large organizations, it is not without its downsides especially for smaller companies. If used with care and to the extent necessary, working with data in Cloud can immensely benefit for all types of businesses [22].

Cost Efficient

Cloud computing is probably one of the most cost efficient method to use. Traditional desktop software with multiple users costs companies a lot in terms of economy. The Cloud, on the other hand, is available at much cheaper rates and hence, can drastically lower the company's IT expenses. Besides this the pay-as-you-go and other scalable options available makes it very reasonable for the business in use.

Almost Unlimited Storage

Storing information in the Cloud gives us almost unlimited data storage capacity. Hence, we no more need to think about running short of storage space or increasing our current storage space capacity.

 Backup & Recovery

Since all our critical data is stored in the Cloud, so backing it up and restoring the same is relatively much easier in Cloud than storing the same on a physical device. Hence, this makes the entire process of backup and recovery much simpler than other traditional methods of data storage.

 Automatic Software Integration

In Cloud, software integration is usually something that occurs automatically. It means that we do not need to take additional efforts of customizing and integrating our applications as per our preferences. Not only this, Cloud computing allows us to customize our options with great ease. One can easily handpick just those services and applications that they think will best suit their particular enterprise.

 Easy Access to Information

Once we register ourselves in the Cloud, we can access our information from anywhere, where an Internet connection is available. This convenient feature lets us to move beyond time zone and geographic location issues.

 Quick Deployment

Lastly and most importantly, Cloud computing give us the advantage of quick deployment. Once we opt for this method of functioning, our entire system can be fully functional within few minutes.

2.5 Issues in Cloud Computing

Concerns related to Cloud computing are given and surveyed by various researchers from Cloud domain, some of them are [27].

 Security

As Cloud computing is gaining popularity, concerns about the security issues introduced through adoption of this new model. However, in Cloud, your data will be distributed regardless of where your base repository of data is ultimately stored. Industrious hackers can invade virtually any server, and there are the statistics that show that one-third of breaches result from hackers and attackers [24].

 Privacy

Cloud computing uses the virtual computing technology, users personal data may be scattered in various virtual data center rather than stay at the same physical location, even across the countries borders, hence data privacy protection will face the controversy of different countries legal systems [25].

 Availability

Like any external service cloud computing also requires a high degree of availability to prevent an adverse impact on business operations. When using a Cloud computing for any business critical operations, consumers must evaluate the risk associated with loss of connectivity to the CSP.

 Integrity

Integrity in simple terms refers to the fact that data cannot be modified by unauthorized person. An organization doesn't want its customers to see data of other customers stored in same server but it is also not wanted that they can alter data uploaded by customers.

 Reliability

The Cloud servers also have the same problem as our own resident servers; they experience downtimes and slowdowns, what the difference is that users have a higher dependent on CSP in the Cloud computing model.

 Legal Issues

Various legal issues like trademark infringement, security concerns and sharing of proprietary data resources arises with Cloud computing. The question comes that „who is in possession of the data" and what happens if provider customer relationship ends?

 Vendor Lock-In

Most Cloud platforms and services are proprietary, means they are built on the specific standards, tools and protocols developed by a particular vendor for its particular Cloud offering [18]. This will make migrating off a proprietary Cloud platform prohibitively complicated and expensive.

 Compliances

Many regulations pertain to storage and usage of data require regular auditing and reporting trails, so Cloud providers must enable their customers to comply appropriately with these regulations. The data centers maintained by Cloud providers must also be subject to compliance requirements.

CHAPTER 3

CRYPTOGRAPHY & NETWORK SECURITY OVERVIEW

Nowadays information is one type of asset that has value like other asset and we need to be secured it from attackers.

To be secured, data needs to be hidden from unauthorized access, protected from unauthorized change and always available to an authorized entity when it is needed. A few decades earlier, the information is collected by an organization and it was stored on physical files. Only a few people had right to access the confidentiality of the file and in the same way only a few people were right to change the content of the files. At least one person had right to access the file at all times.

With the adventure of computer, data storage become electronically. Instead of being storage on physical file, now data was stored in computers. The three security requisite however did not change. The files stored computers also required confidentiality, integrity and availability.

There in last two decades, computer network make a revolution in the use of information. Information is now distributed all over world. An authorized people can send and access the data from remote area using computer network.

In this chapter, we give the overview on network security, It first gives the idea of security attack, and then describe the cryptography terminology which is used keep to be confidentiality of data and also describe the few cryptographic algorithm which provide the strong security of data. At last we discuss the how the cryptographic techniques used on cloud environment.

3.1 Security Goals

Let us first we discussed three security Goals: Confidentiality, Integrity and Availability.

3.1.1 Confidentiality

It defines the only sender and intended recipients should be able to access the content of the message.

3.1.2 Integrity

Integrity specifies the extent to which an application shall ensure that its data does not get intentionally corrupted or modifies through unauthorized creation, modification and deletion. Its objective is to ensure that data and communication can be trusted.

3.1.3 Availability

Availability means resources are always accessible for authorized entity. The unavailability of information always leads to harm for organization as the lack of integrity or confidentiality.

3.2 Attacks

There are main two attacks exists when data store on cloud server those are:

3.2.1. Inside Attack:

In inside attacks is malicious activity which is preceded by TPA or CSP itself. They change the confidential data either by deleting or by manipulating the data on the server side. They get the information and can explore to the external parties, who can exploit it.

3.2.2. Outside Attack:

In outside attack the malicious activity is preceded by any outsider or unauthorized entity not from cloud. The unauthorized entity is like an attacker, software, hardware etc, who

can change the data internally and can make use of any type or he may can exploit the information by disclose to other persons.

Our three goals of security (confidentiality, Integrity, Availability) can be threatened by security attacks

3.3 Attacks Threatening Confidentiality

3.3.1 Snooping

Snooping refers to unauthorized person access the data or intercept the data and Use the data for her own benefit. To prevent this type of malicious activity, data can be sent unreadable form by using cryptography.

3.3.2Traffic Analysis

Attacker generally monitoring the online traffic and analyzed the past data, and try to find the address of intended sender and user. She can collect the all information to help her guess the nature of data and transaction.

3.4 Attacks Threatening Integrity

3.4.1 Modification

Attackers try to intercept the message and modified it to her benefits. Sometime attacker only deletes or delays the message to data to harm the entity or to benefit from it.

3.4.2 Masquerading

Masquerading will be happens when the attacker personates somebody else, and use her data for her own benefit.

3.4.3 Replaying

It is another type of attack. In this attack, attacker obtained the copy of message and later tries to replay it for her own benefit.

3.4.4 Repudiation

It is different type of attacks from others because it is performed between the sender and receiver. Later the sender deny that she has sent the message and receiver deny that he has received the massage.

3.5 Attack Threatening Availability

3.5.1 Denial of Service

DOS is very common attack. It may fully interrupt the service of the system.

In this attack, attacker sends o many fake requests to the server that the server crashes because of heavy load. The attacker could intercept the all responses from the server side and delete them, making the client to the server is not responding.

3.6 Cryptography

Security can be achieved through the Cryptography. Cryptography word is Greek origin which means "Secrete writing". It is terminology where data will be transformed one form to another form, and make them to secure from attackers. When data sends it will be encrypted using secrete key, is called encryption and when data is to be received then it will be decrypted using secrete key by receiver, is called decryption. Today cryptography is defined as involving three mechanisms these are:

3.6.1 Symmetric-Key Cryptography

In Symmetric-Key Cryptography both parties use the same secrete key.

Sender uses single key for encryption process and receiver also uses same key for decryption process. There are many algorithm based on single secrete key is used for security of data, which is more reliable and efficient than classic method.

DES, AES, IDEA, Blowfish, Twofish, RC4, RC5 etc. are the example of Symmetric- Key Cryptography.

DES takes a 64 bit input and creates 64 bit ciphertext, and also using same secrete key it creates 64 bit plaintext. In both process 56 bit cipher key is used for encryption and decryption. Initially 64 bit plaintext permutes according to predefined method. That have to processed 16 round and finally permutes the cipher and get 64 bit cipher text.

AES is similarly like DES, here only rounds are different .It has defined different three type of version with 10, 12, 14 rounds and each version uses different key size 128, 192,256. But round key is always 128 bits.

Ashwak ALabaichi, Faudziah Ahmad, Ramlan Mahmod have analyzed the security of Blowfish algorithm and it can be concluded that It presents the good avalanche text from the second round [28].

3.6.2 Asymmetric-Key Cryptography

In Symmetric-Key Cryptography both parties use different key. Sender uses the reciever's public key for encryption process and receiver use his own private key for decryption process. Symmetric-Key cryptography and Asymmetric-Key Cryptography both are compliment of each other. In Symmetric-Key Cryptography shared the privacy between to entity while in Asymmetric-Key Cryptography the privacy is personal.

There are many cryptosystem works on Asymmetric-Key Cryptography. RSA, Rabin, ElGamal, Elliptic curve cryptosystem etc. are the example of Asymmetric-Key Cryptography.

3.6.3 Hashing

Hashing is one type of function which is used for authentication of the message. It takes arbitrary length of message and creates fixed length of message digest. It is used to provide check values and also provide data integrity.

3.7 Security on cloud Environment

Cloud computing is in demand nowadays because of its usability and reliability. It provide us better platform for sharing data, messages, hardware, software and so on without fear of losing data. For protection of data on cloud firstly we should have to

analyzed or identified the Security Requirement Functionalities. Again these identified Security Requirements can be prioritize & managed and finally passed over to the Security Design phase so that proper design decisions based on these Security Requirements should be taken in cryptography based cloud models.

The detailed description about these Security Requirements with the associated Security Functionalities are given below:

- **Identification & Authentication**

Identification requirement specifies the extent to which a Cloud system shall identify its external users before interacting them, like applying turing test etc. Similarly authentication requirement is used to verify the identity of externals what they claims to be before interacting by using attributes like User ID or Password etc.

This security requirement associates with many functionalities.

- *User Identification (UID)*: It defines conditions based on which users are required to identify themselves before performing any action which demands user interaction. E.g.

  Cloud Storage shall apply turing test on customers and users. Or Cloud Storage shall use multidimensional attributes for identification.

- *User Authentication (UAU)*: It defines the user authentication mechanism and required attributes on which the mechanism must be based. E.g.

  -'Cloud Storage shall use combination of UserID and Password for Authentication.' Or

  - 'Cloud should use biometrics attributes for Authentication.'

- *Authentication Failures (AFL)*: This requirement deals with defining some limit on unsuccessful authentication attempts or necessary action when authentication fails. E.g.

  - 'Cloud Storage should not allow more than three consecutive wrong authentication attempts.' Or

- ‘Cloud shall notify the security administrator in case of consecutive wrong attempts.’

- *Limitation on scope of selectable attributes (LSA)*: This requirement applies a limit on the scope of security attributes related to a session that a user select during a session establishment. E.g.

- ‘The Cloud Storage shall not allow three months old password to gain access.’
- ‘Cloud shall regularly change the key size used for encrypt transfer.’

- *Limitation on multiple concurrent sessions (MCS)*: This Security Requirement applies a limit on the number of session occurring concurrently that belongs to a same user. E.g.

- ‘Cloud Storage shall only allow single session at a time from same user.’
- ‘Cloud shall record locations used during multiple session from same user.’

- *System access banners (TAB)*: This requirement specifies the need to display advisory warning related to system use before a session to the users. E.g.

- ‘Cloud shall regularly notify customers to change login details.’
- ‘Cloud shall warn customers about remaining unsuccessful attempts.’

- *System access history (TAH)*: This requirement deals with the need to display a history of successful and unsuccessful attempts to user‟s account after the establishment of a session. E.g.

- ‘Cloud Storage shall display last login attempts to all customers.’
- ‘Cloud Storage should maintain archives of last 1 month login attempts details.’

- *System session establishment (TSE)*: It deals with accepting or denying a users request for session establishment based on certain attributes. E.g.

- ‘Cloud Storage shall temporarily suspend services for specific customer in case of doubtful login attempt.’
- ‘Cloud Storage allow session establishment only after verifying every security Attribute related to customer.’

- **Authorization**

Authorization requirement specifies the extent to which the Cloud system verifies the usage privileges and access restrictions of authenticated users and application. This requirement prevents unauthorized users from obtaining access to inappropriate data or services.

Associated functionalities with this Security Requirement are:

- *Security management roles (SMR)*: It deals with the control over the assignment of different roles to various users in a system. E.g.

  - 'Cloud Storage shall have predefined roles for employees.'
  - 'Cloud shall impose restrictions based on roles.'

- *Security Attribute Expiration (SAE)*: This requirement deals with the assignment of time limits for the validity of various security attributes.

  - 'Cloud Storage shall terminate session if unattended for 10 minutes.'

- *User-Subject Binding (USB)*: This requirement creates and associate user"s security attributes, totally or partially to a subject which acts on user"s behalf. E.g.

  - 'Cloud Storage shall relate the device used to gain access with UserID.'
  - 'Cloud shall verify customers device also before establishing sessions.'

- *Session locking and termination (SSL)*: This requirement deals with the capability of user initiated locking, unlocking and termination of session.

  - 'Cloud Storage should provide function to temporarily suspend services to customers.'

- **Immunity**

Immunity requirement specifies the extent to which a Cloud system shall protect itself from undesirable programs like viruses, worms etc. from destroying or damaging the data and system applications.

Associated functionalities with Immunity Security Requirement are:

- *Testing of external entities (TEE)*: This requirement allows the SSF to test one or more external entities (like applications running on system, hardware, software etc.). E.g.
  - 'Cloud Storage shall test critical devices before communication.'
  - 'Cloud shall report security administrator if error detected.'
- *SSF self test (TST)*: It deals with the self testing of SSF by the system, which can be performed at startup, periodically or at request from authorized user. E.g.
  - 'Cloud Storage should test its virus chest for updates periodically.'
  - 'Cloud shall test connection between devices after startup.'
- *Revocation (REV)*: This requirement deals with the security attributes revocation for variety of entities within a system. E.g.
  - 'Cloud Storage should delete information of customers who unsubscribe services.'
  - 'Cloud Storage shall scrap left over employee's access credentials.'
- *Import from Outside (ITC)*: This requirement defines the mechanism for either protecting security attributes or not for a user data when importing into the system from outside. E.g.
  - 'Cloud Storage shall allow customers to select encryption method at client side before uploading their data.'

➢ **Integrity**

Integrity requirement specifies that a Cloud shall protect its data and communication from any unauthorized modification or deletion. Its main objective is to ensure that the communication and data can be trusted.

Associated functionalities with Integrity Security Requirement are:

- *Data Authentication (DAU)*: Data authentication means that an entity is responsible for the authenticity of information. This requirement specifies a

method to verify the authenticity of static data, that the content has not been forged. E.g.

- 'Cloud Storage shall verify the owner of data before storing.'
- 'Cloud shall immediately remove unauthentic data.'

- *Internal System Transfer (ITT*): It specifies the extent to which user data is protected when it is transferred between various parts of a system through internal channels. E.g.

- 'Cloud Storage should use reliable channel for internal transfer of data.'

- *Stored Data Integrity (SDI)*: It specifies the protection of user critical data while it is stored within the boundary of a system. It differs from ITT which protects the integrity of user data while being transferred within a system. E.g.

-'Cloud Storage shall regularly check the stored customer data for any Unauthorized modification.'

- *Rollback (ROL)*: This requirement provides the ability to undo the effect of an operation in a system to ensure the integrity of user data. E.g.

- 'Cloud Storage shall preserve the status of data in timely manner.' Or
- „Cloud Storage shall restore the previous state of customer data if unauthorized modification detected.'

➢ **Intrusion Detection**

Intrusion requirement specifies the extent to which a Cloud shall perform detection and recording of intrusions or modifications by unauthorized or authorized persons. It may include potential response activities like security alarms etc. in case of intrusion.

Associated functionalities with this Security Requirement are:

- *Replay detection (RPL):* This requirement deals with the detection and prevention of replay actions from various types of entities. E.g.

- 'Cloud Storage shall discard multiple requests within short time to prevent Denial of Services.'

- *Testing of external entities (TEE):* This requirement allows the SSF to test one or more external entities (like applications running on system, hardware, software etc.). E.g.

  - 'Cloud Storage shall test customer device after session start.'
  - 'Cloud shall immediately discard device if error detected.'

- *Revocation (REV)*: This requirement deals with the security attributes revocation for variety of entities within a system. E.g.

  - 'Cloud Storage shall discard access credentials of employees after they left.'

- *Information flow control policy (IFC)*: This requirement identifies the information flow control policy and also defines the scope of control for each information flow control by identifying the subject, information and operation under control of policy. For e.g.

  - 'Cloud Storage shall select reliable path for information flow.'

- *Information flow control functions (IFF)*: It describes the rules related to specific function that implements the information flow control policy identified in IFC. E.g.

  - 'Cloud Storage shall test all nodes before actual transfer begins.'

➢ **Non Repudiation**

Non repudiation security requirement specifies that Cloud shall prevent the sender and receiver from denying their involvement in communication at later stage. Its objective is to maintain records about critical involvement of customers to prevent them from denying.

Associated functionalities with Non-Repudiation Security Requirements are:

- *Non-repudiation of Origin (NRO)*: This requirement specifies that the originator of information cannot deny after sending the information. It requires a method to provide evidence of the origin to receiver. E.g.

  - 'Cloud Storage shall store information of every data upload action.'

- *Non-repudiation of Recipient (NRR)*: It specifies that the recipient of information cannot deny after receiving information. It requires a method to provide evidence of receipt to the sender. E.g.

- 'Cloud Storage shall store recipient for every data downloaded.'

➢ **Privacy**

Privacy security requirement specifies the extent to which Cloud system shall protect the customer's critical data stored on its server or during communication from any unauthorized person or attackers. Its objective is the protection customer's data, identity and actions so that it became unobservable to others.

Associated functionalities with Privacy Security Requirement are:

- *Cryptographic Key Management (CKM)*: These requirements specify that the cryptographic keys must be properly managed throughout its life cycle like key generation, distribution and destruction. E.g.

-'Cloud Storage shall transfer the encryption keys to customer through secure channel.'

- *Cryptographic Operations (COP)*: It specifies that the cryptographic operations must be implemented in accordance with a specified algorithm and key size. Various cryptographic operations are encryption / decryption, digital signature verification, checksum generation and verification etc. E.g.

- 'Cloud Storage should not public the algorithm used for encryption.'

- *User data Confidentiality Transfer Protection (UCT)*: This requirement ensures the confidentiality of user data when it is transferred from a system to another product using an external channel. E.g.

- 'Cloud Storage should always send encrypted data to customers.'

- *Import from Outside (ITC):* This requirement defines the mechanism for either protecting security attributes or not for a user data when importing into the system from outside. E.g.

- ‘Cloud Storage shall allow customers to select encryption method at client side before uploading their data.’

- *Internal System Transfer (ITT)*: It specifies the extent to which user data is protected when it is transferred between various parts of a system through internal channels. E.g.

- ‘Cloud Storage should also encrypt data when transferred internally.’

- *Anonymity (ANO)*: It ensures that a user without disclosing its identity may use a resource or services in a system. E.g.

- ‘Cloud Storage shall verify identity in encrypted form.’

- *Pseudonymity (PSE)*: This requirement specifies that a user without disclosing its identity may use a resource or service, but can still be accountable for that. E.g.

- ‘Cloud Storage shall record all usage details of customers in encrypted form.’

- *Unlinkability (UNL)*: It ensures that multiple use of resources and services are allowed to a user, such that others are unable to link these uses together. E.g.

-‘Cloud Storage should encrypt the service usage links of customers.’

- *Unobservability (UNO)*: This requirement ensures that a user may use resources and services, such that others are not able to observe this utilization. E.g.

- ‘Cloud Storage should hide the customer usage pattern from others.’

- *Trusted Path (TRP)*: This requirement expresses the need to implement and maintain a trusted communication between user and the system. E.g.

- ‘Cloud Storage shall selected secure nodes in a path to customer.’

➢ **Security Auditing**

Auditing security requirement specifies the extent to which Cloud system shall allow security auditors to inspect the system behavior and status from security point of view. Associated functionalities with Security Auditing Requirement are:

- *Security Audit Automatic Response (ARP)*: This requirement defines the response that should be taken in case of security violation. E.g.

- ‘Cloud Storage should terminate session in case of violation.’

- *Security Audit Data Generation (GEN)*: This requirement defines the need for recording the occurrence of security events by the system. E.g.

- ‘Cloud Storage shall continuously record all unsuccessful attempts.’

- *Security Audit Analysis (SAA)*: It defines the need for automated monitoring of system activities and audit data for identifying security violation in system. E.g.

- ‘Cloud Storage shall regularly monitor access details of customers.’

- *Security Audit Review (SAR)*: It specifies the need of audit tools that should be available to authorized users only to help them in reviewing audit data. E.g.

- ‘Cloud Storage shall have automated tools for analyzing large audit data.’

- *Security Audit Event Storage (STG)*: It says that the system should be able to create and maintain a secure audit trail which guarantees availability of audit data. E.g.

- ‘Cloud Storage shall have feature to generate audit data when needed by Auditor.’

➢ **Survivability**

Survivability requirement specifies that a Cloud system shall provide the basic functionalities or either fails gracefully even when some components or devices have been destroyed intentionally or naturally. Its objective is to survive the intentional component destruction.

Associated functionalities with Survivability Security Requirement are:

- *Fault Tolerance (FLT)*: This requirement ensures that the system will provide basic functionality in the event of failure also. E.g.

- ‘Cloud Storage have backup ready for providing basic services.’

- *Priority of service (PRS)*: It specifies that resources with high priority will always be accomplished without any delay caused by low priority activities. E.g.

- ‘Cloud Storage shall protect customer data first in the event of security attack.’

- *Resource allocation (RSA)*: This requirement allows the system to control the resource utilization such that denial of service will never occur. E.g.

- 'Cloud Storage shall not allow full load on its data servers.'

- *Fail Secure (FLS)*: This requirement ensures that the system will always enforce its security requirements in the event of failure as identified in the SSF. E.g.

- 'Cloud Storage shall immediately notify the security administrator to replace device if it fails.'

➢ **Recoverability**

Recoverability security requirement specifies the extent to which Cloud system shall recover the data and system after the failure happens. Data recoverability deals with data correction after authorized or unauthorized modification whereas system recoverability specifies that a system recovers to a secure state after failure or modification.

Associated functionalities with Recoverability Security Requirement are:

- *Trusted recovery (RCV)*: This requirement specifies that the SSF can successfully recover the system after discontinuity of operations. E.g.

- 'Cloud Storage shall have proper mechanism to recover customer data in the event of failure.'

- *State synchrony protocol (SSP)*: This requirement ensures that various parts of a system have properly synchronized their states after some security related action in a Cloud system. E.g.

-'Cloud Storage shall synchronize their devices after recovery from security attack.'

- *Rollback (ROL)*: This requirement provides the ability to undo the effect of an operation in a system to ensure the integrity of user data. E.g.

-'Cloud Storage restores data to its previous state if unauthorized modification is detected.'

- **Physical Access Protection**

Physical access protection requirement specifies that a Cloud system shall protect its data centers and itself from unauthorized physical access, damage, theft, hardware replacement or sabotage.

Associated functionalities with Access Protection Security Requirement are:

- *Access Control Policy (ACC)*: This requirement identifies the access control policy and defines the scope of control of the policies on the object. E.g.

  -'Cloud Storage shall cover every employee in access control policy to data centers.'

- *Access Control Function (ACF)*: This requirement describes the rules related to specific functions that are implemented by the access control policy defined by ACC. E.g.

  -'Cloud Storage shall allow only limited employees to enter inside data centers.'

- *SSF physical protection (PHP)*: This requirement specifies the restriction applied on unauthorized physical access and physical modification to the SSF. E.g.

  -'Cloud Storage shall immediately raise alarm if security breach is detected in data centers.'

- **System Maintenance**

This security requirement specifies the extent to which Cloud system shall protect itself from any accidental authorized modification during maintenance or updates. It also includes management of security features and attributes.

Associated functionalities with System Maintenance Security Requirement are:

- *Management of Security Attributes (MSA)*: This requirement allows the control over the management of security attributes by an authorized users like modifying attributes or viewing etc. E.g.

  - 'Cloud Storage shall not allow any employee to view customer data.'

- *Management of Security Functionality Data (MTD)*: It allows the control over the management of security functionality data like audit information and configuration parameters by an authorized user. E.g.

  - 'Cloud Storage shall encrypt audit data and allow only authorized Auditors to decrypt them.'

- *Internal System Transfer (ITT)*: It specifies the extent to which user data is protected when it is transferred between various parts of a system through internal channels. E.g.

  -'Cloud Storage should also encrypt data when transferred internally.'

  -'Cloud shall distribute keys to authorized persons to decrypt security functionalities data.'

So all researchers should have to keep in mind above explained all security requirements functionalities and take a best decision for developing a model in the perspective of data security.

CHAPTER 4

PROPOSED METHODOLOGY

4.1 Block Status Table

The Block Status Table (BST) is one type of data structure; It is implemented using linked list. BST is used to access the outsourced cipher from the cloud environment as well as checked the duplication through message digest. It has two column such as MD_j and BNj_j, MD_j is the message digest of data block j and BN_j is the data block number. Initially the data owner fills the table entries as BN_j=MD_j= j.

4.2 Proposed Symmetric Key Cryptographic Algorithm

4.2.1 Encryption

Step 1: Take input from the data owner and divide the data into 64 bytes block each and store it in the array A.

Step 2: Generate the ASCII value of each character and store it in a new array B.

Step 3: For each ASCII value compute the modulo 64 and store the corresponding remainder value in array C.

Step 4: If two or more values of remainder in array C are same then replace the latter value(s) with one of the unused values between 0 to 64 taken in increasing order.

Step 5: Take the first value in array C and call it Y. Replace the first value in array B with the value at index Y in array B. Replace other elements of B in the same way.

Step 6: Convert the ASCII values of modified array B into characters to get the cipher text.

Step 7: Generate the corresponding binary value of each remainder (Binary value should be 6 digits e.g. for decimal 16 binary number should be **0**10000).

Step 8: Reverse the 6 digit's binary number.

Step 9: Take a 3 digits divisor (>=100) as the **Key.**

Step 10: Divide the reversed number with the divisor.

Step 11: Store the remainder in first 2 digits & quotient in next 4 digits (remainder and Quotient wouldn't be more than 2 digits and 4 digits long respectively. If any of these are less than 2 and 4 digits respectively we need to add required number of 0s (zeros) in the left hand side. So, this would be the encrypted array C.

Step 12: Send the array C and cipher text.

4.2.2 Decryption

Firstly decrypt the encrypted array C and then decrypt the cipher text.

Step 1: Multiply last 4 digits of the encrypted array C by the Key.

Step 2: Add first 2 digits of the encrypted array C with the result produced in the previous step.

Step 3: If the result produced in the previous step i.e. step 2 is not a 6-bit number we need to make it an 8- bit number

Step 4: Reverse the number to get the original array C i.e. remainder array.

Step 5 :Create a new array D. Take the first value, say X from array C. Now put the first value from array B at an index value X in array D. Put other values in array D in the similar way. The resultant array D will represent the original plain text.

4.3 Proposed Cryptographic Hash Function Algorithm.

Step 1: Assign the numeric value to each alphabet (e.g A=0, B=1, C=2……Z=25, space=26).

Step 2: Take 64 bytes block input from user.

Step 3: Divide it into sub blocks of 8 bytes each.

Step 4: For each character in every sub block, multiply it's numeric value with its index value in that sub block. The resultant values obtained for each character in the sub block are added to get a single value for one sub block

Step 5: Convert the values obtained for sub blocks into Hexadecimal.

Step 6: Concatenate these Hexadecimal values of each sub block to get the message digest.

4.4 Proposed Framework

Authentication, integrity, access control, encryption, integrity checking and data masking are some of the data protection techniques. Cryptography is the one of the efficient technique for data security in cloud computing. This includes the design and implementation of an efficient encryption and decryption algorithms. In symmetric cryptography, before outsourcing data to cloud server is encrypted into cipher text using secret key and later user decrypted using same shared secret key and also used the hashing function for authentication as well as removing the data duplication.

In proposed system I have focused on preserving the outsourced as a security aspect and remove the duplication of storage file from client location to server location. Due to this reason I proposed a highly efficient encryption technique and hash function which is used in local server before sending the data to trusted third party auditor (TTPA). Before sending the data, date will be divided into block, and each block contains the 64 byte of data. Each block is encrypted using my proposed encryption technique and each block creates fixed number of message digest, and prepare a BST table for encrypted file.

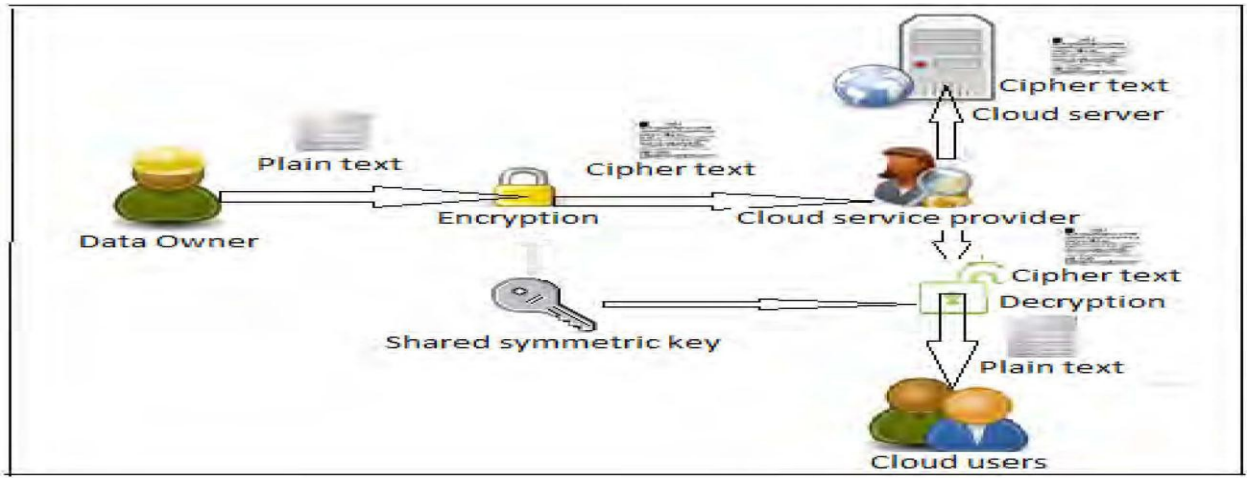


Figure 8: Block Diagram or Data Encryption and Decryption in Cloud System

Then send the table, key and encrypted file to TTA. Table which contains the information of each block (such as block number, status of block and so on)

and massage digest of particular block. When end user request the access the data that time request will be send over two places, at TTPA and at cloud service provider (CSP). TTPA firstly authenticates the user and sends the signal to CSP in the form of negative or positive. If signal is positive, then CSP sends the particular file to end users and TTPA will also send the particular table which stores the information regarding file. End user calculate the hash value of particular message which have got from CSP and compare that value from TTPA table which contain the hash value. If both of the value is matched then message is authenticated and then decrypt the message using decryption algorithm.

4.5 Proposed Model

Our proposed cloud data storage system model for secure data access sequences are explained in the above Figure. The following sequence numbers are represented for data storage and access operations in cloud server.

I. The data owner splits the source file in to the blocks of 64 characters and encrypt all the blocks using above encryption algorithm as well as create the massage digest of each block and prepare the Block Status Table (BST) for encrypted blocks, then send the encrypted file, key, BST to the Trusted Third Party (TTP) auditor.

2. The TTP kept the message digest of each message and send only encrypted file and BST to the cloud server for storage.

3. The end user sends the request for data access to both TTP and cloud server.

4. TTP verifies the end user, if the user is verified then, it send the authorization signal to the cloud server.

5. TTP send the message digest of data and encrypted file to the end user.

6. Cloud server send the BST and encrypted file to the user.

7.End user calculate the hash values of encrypted file received from the cloud server then verifies with hash values received from the TTP. If both values are verified then user gets a data decryption key and decrypt the data blocks.

CHAPTER 5

IMPLEMENTATION AND RESULT ANALYSIS

5.1 Tools Used

We have used the following tools during the development of our project.

- **Microsoft Visual Studio:** It is an integrated development environment (IDE) from Microsoft. It is used to develop computer programs for Microsoft Windows, as well as web sites, web applications and web services. Visual Studio uses Microsoft software development platforms such as Windows API, Windows Forms, Windows Presentation Foundation, Windows Store and Microsoft Silverlight. It can produce both native code and managed code.
- **C Sharp (C#):**It is a multi-paradigm programming language encompassing strong typing, imperative, declarative, functional,generic, object-oriented (class-based), and component-oriented programming disciplines. The language, and implementations thereof, should provide support for software engineering principles such as strong type checking, array bounds checking, detection of attempts to use uninitialized variables, and automatic garbage collection. Software robustness, durability, and programmer productivity are important.
- **Asp.net :** It is an open-source server-side Web application framework designed for Web development to produce dynamic Web pages. It was developed by Microsoft to allow programmers to build dynamic web sites, web applications and web services.
- **My SQL Server:** My SQL Server has been used to make relations for our development tool. The main theme to use access is it is a very light weight database and provides all the basic database utilities that we need in our project. We do not want any security feature to the database hence we have used this database.

5.2 Snapshots

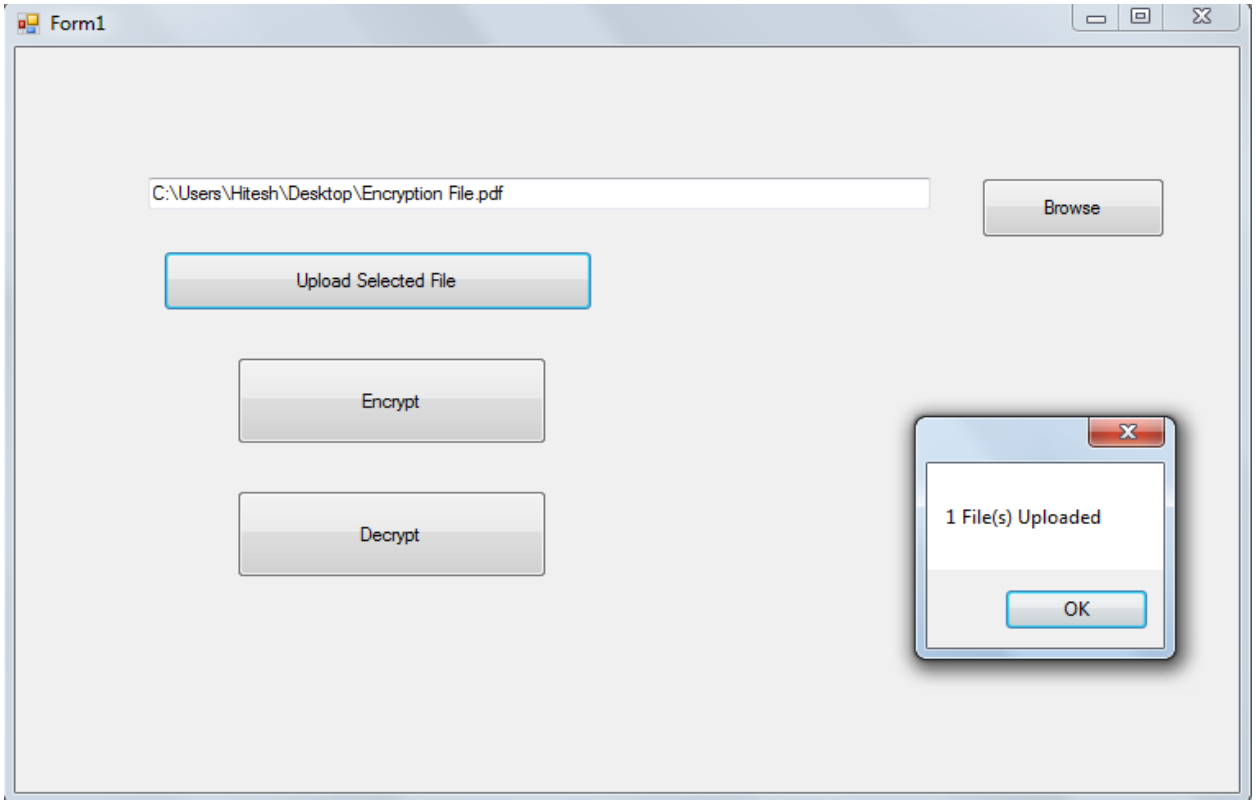


Figure 9: Client Side Encryption

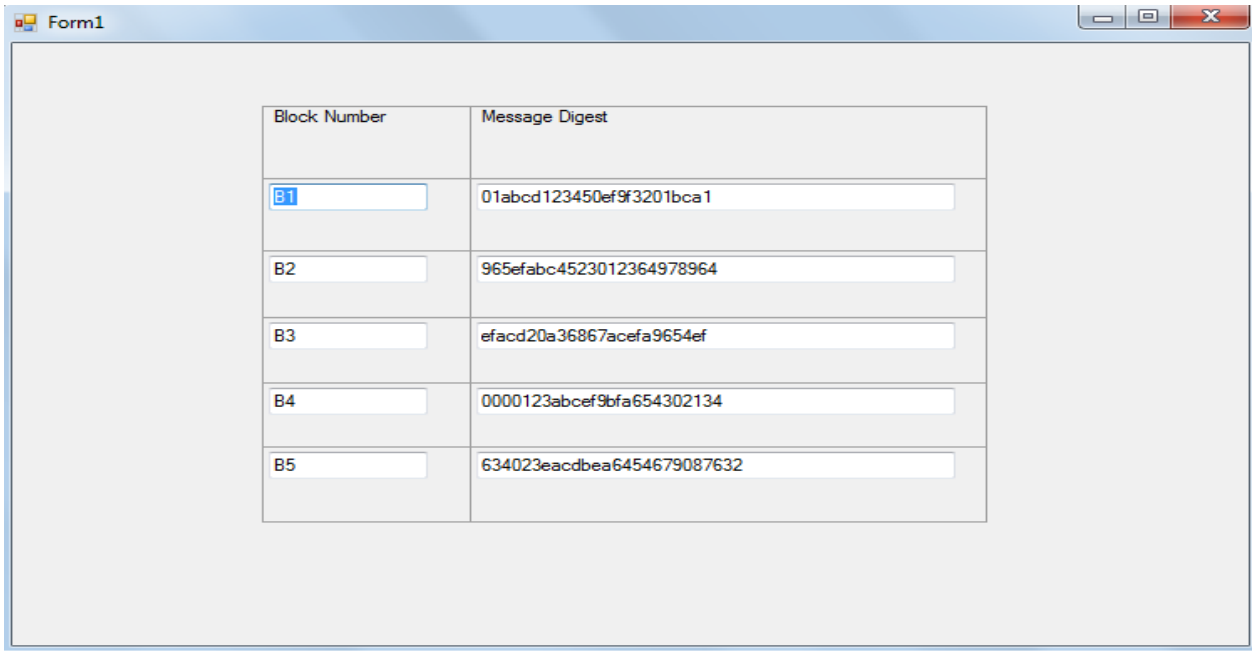
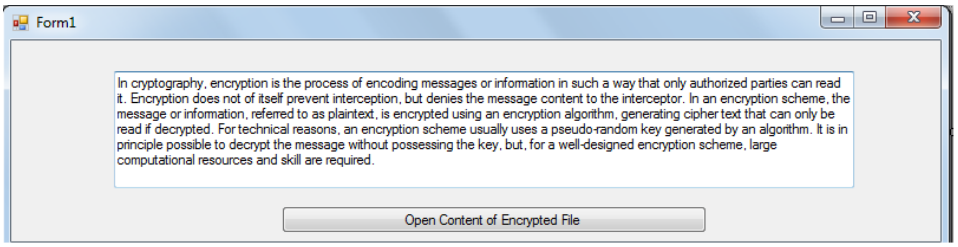


Figure 10: TTPA Table1



Content of Encryption File

In cryptography, encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not of itself prevent interception, but denies the message content to the interceptor. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, generating cipher text that can only be read if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-random key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, large computational resources and skill are required.

Figure 11: Decryption

5.3 Objectives

Data security for outsourcing and accessing data from cloud server, our proposed security model achieves the following objectives.

i. Lightweight overhead: design a lightweight computation, storage and communication overhead for verification of authorized cloud users and access the cloud date.

ii. Block level data operation: design an efficient block level encrypted data operations.

iii. Confidentiality and integrity: design an efficient data encryption before outsourcing to cloud server and decryption algorithms at user side.

5.4 Advantages of Proposed Algorithm.

To retain control over data in cloud environment, the encryption and strong key management is more important to the organization to meet the security challenges. The benefits of the encryption in cloud environment are;

1. Encryption ensuring the privacy of the organization data, while encrypted data is in the transmission, in use and at storage location

2. Encryption Helps Achieve Secure Multi-Tenancy in the Cloud Encrypting data in the cloud and holding encryption key data owner can avoid the cloud service provider to access the data.
3. Encryption Provides Confidence of data backups are safe in cloud environment from the breached party.
4. The Algorithm is very simple in nature.
5. There are two reverse operations present in this algorithm which would make it more secured.
6. CRC checking in receiving ends is easier.
7. The file is divided into blocks and confidentiality is emphasized on every character level of a block.

CONCLUSION AND FUTURE ENHANCEMENT

Usage of Cloud storage services basically means uploading critical data on third party storage servers where no prior relationship has been established based on trust. Cloud customers who upload their personal data on Cloud want to be sure that only authorized persons can access their data, which may exclude CSP also. Nowadays large number of users and businesses are adopting Cloud computing due to its enormous benefit, but this adoption also brings many security concerns as discussed earlier in Cloud system.

We have proposed an efficient data encryption and data decryption algorithm to protect the outsourced sensitive data in cloud computing environment. With data encryption, data owner can utilize the benefits of file splitting to reduce storage and computational overheads. On the other hand, to reduce the burden of data owner, trusted third party is introduced for verification of authorized users to access the data from cloud server. We demonstrate the performance of encryption and decryption algorithms in terms of data privacy, computational efficiency and effectiveness of the cloud. Keeping this goal in mind the proposed algorithm has been designed in a quite simple manner but of-course not sacrificing the security issues. A single key is used for both encryption and decryption i.e. it is fallen under secret key cryptographic algorithm. But as public key cryptography is more secured then secret key cryptography our next task would be to develop and design a public key cryptographic algorithm in a simple manner as it is done in this thesis and also propose a secure model with more functionality, which is more better than previous one.

REFERENCES

[1] Nandita Sengupta, Jeffrey Holmes , Designing of Cryptography Based Security System
for Cloud Computing, 2013 International Conference on Cloud & Ubiquitous Computing & Emerging Technologies

[2] Aws Naser Jaber, Mohamad Fadli Bin Zolkipli, Use of Cryptography in Cloud Computing, *2013 IEEE International Conference on Control System, Computing and Engineering, 29 Nov. - 1 Dec. 2013, Penang, Malaysia*.

[3] Kajal Chachapara, Sunny Bhadlawala, Secure sharing with cryptography in cloud Computing, *2013 Nirma University International Conference on Engineering (NUiCONE).*

[4] Kirti Gupta, Dr. Shailendra Narayan Singh, Methods for Maintaining Security on Cloud of Stored Data, *978-1-4799-4236-7/14/$31.00 c_2014 IEEE.*

[5] J.P. Martin-Flatin, EPFL, Challenges in Cloud Management*, IEEE cloud computing published by the IEEE computer society.*

[6] Mohamed Hamdi, Security of Cloud Computing, Storage, and Networking, *978-1-4673-1382-7/12/$31.00 ©2012 IEEE.*

[7] Kamlesh Kumar Hingwe, S. Mary Saira Bhanu, Sensitive Data Protection of DBaaS using OPE and FPE, *2014 Fourth International Conference of Emerging Applications of Information Technology.*

[8] Chao Yang, Jian Ren and Jianfeng Ma, Provable Ownership of File in De-duplication Cloud Storage, *Globecom 2013 - Communication and Information System Security Symposium.*

[9] Feng Zhao , Chao Li , Chun Feng Liu, A cloud computing security solution based on fully homomorphic encryption.

[10] Zhang-Tong, WU-Qi, LIU-Wen, CHEN-Liang, Homomorphism Encryption Algorithm for Elementary Operations over Real Number Domain, *2012 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discover.*

[11] Suresh kumar Aditya, Kavya Premkumar, R.Anitha, Combined Security Framework for Multi-Cloud Environment, *The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014).*

[12] Fang Liu, Wee Keong Ng, Wei Zhang, Encrypted Association Rule Mining for Outsourced Data Mining, *2015 IEEE 29th International Conference on Advanced Information Networking and Applications.*

[13] Chun-I Fan, Shi-Yuan Huang, and Wen-Che Hsu, Hybrid Data Deduplication in Cloud Environment.

[14] V.Nirmala, R.K.Sivanandhan, Dr. R.Shanmuga lakshmi, Data Confidentiality and Integrity Verification using User Authenticator scheme in cloud, *Proceedings of 2013 International Conference on Green High Performance Computing.*

[15] Priteshkumar Prajapati, Parth Shah, Efficient cross user Data Deduplication in Remote Data Storage*, International Conference for Convergence of Technology – 2014.*

[16] Nesrine Kaaniche, Maryline Laurent, A Secure Client Side Deduplication Scheme in Cloud Storage Environments.

[17] Jian Li1,2, Sicong Chen1, Danjie Song1, SECURITY STRUCTURE OF CLOUD STORAGE BASED ON HOMOMORPHIC ENCRYPTION SCHEME, *Proceedings of IEEE CCIS2012.*

[18] P.Varalakshmi, Hamsavardhini Deventhiran, Integrity Checking for Cloud Environment Using Encryption Algorithm.

[19] Rohit Handa, Rama Krishna Challa, A Cluster Based Multi-keyword Search on Outsourced Encrypted Cloud Data.

[20] Mr. Krunal Patel, Mr. Navneet Singh, Mr.Kushang Parikh, Sendhil Kumar K.S, Dr. Jaisankar N., Data Security and Privacy using Data Partition and Centric key management in Cloud*, ICICES2014 - S.A.Engineering College, Chennai, Tamil Nadu, India.*

[21] Somchart Fugkeaw, Achieving Privacy and Security in Multi-Owner Data Outsourcing.

[22] Cloud computing Wikipedia,https://en.wikipedia.org/wiki/Cloud computing, 2013.

[23] Mell P., Grance T., "The NIST Definition of Cloud Computing", NIST. http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf, May 2013.

[24] Cloud Security Alliance, “Top threats to cloud computing, version1.0”, Tech. Rep., March 2010.

[25] Ren K., Wang C., Wang Q., “Security challenges for the public cloud”, Internet Computing, IEEE, pp 69-73, 2012.

[26] McKendrick J., "Cloud Computing's Vendor Lock-In Problem: Why the Industry is Taking a Step Backward", Forbes, 2011.

[27] Jansen W. A., “Cloud Hooks: Security and Privacy issues in cloud computing”, NIST 44th Hawaii International conference on System Sciences, pp 1-10, 2011.